eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Conceitos:

- ✓ Auditoria
  - ✓ O que é uma auditoria?
  - ✓ Necessidades de uma auditoria
  - ✓ O que pode ser auditado
  - ✓ Testando seu próprio ambiente
  - ✓ Passos para auditoria interna
  - ✓ Auditoria vs Pentest

Auditoria

O que é uma auditoria?

Auditoria é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa ou setor, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Fonte: Wiki

Necessidades de uma Auditoria

Com o excesso de informação transitando por uma rede e cada vez mais rápido, criaram-se muitas técnicas e ferramentas para controle dessas informações.

Muitas vezes, esses controles podem falhar, ou até mesmo o profissional pode cometer erros e estes erros muitas vezes não são percebidos ou sentidos pela gestão.

Existem muitos motivos para se realizar uma auditoria, algumas delas, pegando os profissionais de surpresa.

Um auditor por sua vez, pode realizar diversos tipos de auditorias, até mesmo uma auditoria mais intrusiva para testar os sistemas de gestão e a equipe de monitoramento.

O que pode ser auditado?

Tudo pode ser auditado, desde que tenha autorização para isso.

Na verdade, uma auditoria interna, necessita de autorização dos cargos mais elevados, como gestão do departamento, direção ou até mesmo da presidência.

Em caso de auditoria externa, é necessário um contrato, neste contrato irá delimitar o que pode ser auditado ou não, com multa, rescisão ou até mesmo criminalmente, caso o mesmo não seja seguido a risca.

Nunca pode-se realizar uma auditoria sem a autorização prévia de algum responsável pelo departamento ou empresa, seja ela realizada internamente ou externamente.

Testando seu próprio ambiente

Durante este treinamento, iremos realizar diversas auditorias internas, e com isso, entender as vulnerabilidades que nos cercam, corrigi-las e documenta-las.

Em muitos casos, faremos papel de Pentester e Auditores para verificar se nossos controles de Segurança estão trabalhando conforme o esperado.

Para isso, utilizaremos ferramentas free e técnicas de invasão e evasão para testar os pontos mais críticos de segurança em nosso ambiente.

Nós iremos desenvolver laboratórios controlados, o mais próximo possível de um ambiente real, simular situações básicas, intermediárias e difíceis de se conseguir acesso ou informações sigilosas para o bem de nosso conhecimento.

Não há nada melhor para aquisição de conhecimento do que a realização de testes e o desenvolvimento mais real possível de um laboratório.

Passos para auditoria interna

É natural que muitos de nossos alunos, principalmente aqueles que não trabalham com Segurança da Informação, queiram testar suas habilidades em sua empresa.

Porém, isso não é recomendado sem seguir os passos abaixo:

1. Consiga a autorização do responsável pelo ambiente à ser auditado
2. Deixe os responsáveis cientes que alguns serviços podem deixar de funcionar
3. Jamais faça testes em um ambiente em produção
4. Tenha sempre um backup e um plano recuperação de ambiente
5. Evite sobrecarregar o sistema, principalmente em varreduras
6. Nunca acredite que nada irá acontecer. Até mesmo os ambientes mais estáveis podem causar problemas
7. Faça sempre laboratórios e testes antes de uma auditoria interna.

Auditoria vs Pentest

Esta confusão é mais comum do que se imagina e existem debates enormes sobre a diferença entre esses 2 temas.

Alguns especialistas acreditam que ambos são praticamente iguais, outros que são completamente diferentes na execução e objetivo.

Se levar ao pé da letra, o Pentest é um método que avalia a segurança de um sistema, computador ou uma rede, simulando um ataque real, ao qual, por outro lado, a auditoria apenas faz a verificação das rotinas e procedimentos adotados em uma política de Segurança da Informação.

Algumas empresas começaram a nomear esse tipo de trabalho de forma parecida, quando, além de realizar as rotinas, começaram a realizar os testes de validação de determinadas rotinas.

Auditoria vs Pentest

Vamos dar um exemplo:

Em um determinado ambiente, há uma página de login e senha. Na política de Segurança da Informação, diz que os logins devem contar o nome e o sobrenome do usuário. Por exemplo: João Macedo, sendo assim, seu usuário ficará joao.macedo.

Há outra regra que diz que o usuário deve criar uma senha com no mínimo 8 caracteres, com letras maiúsculas e minúsculas, números e caracteres especiais.

Durante o processo de auditoria, será verificado se tudo está em conformidade e se não há exceções. Porém, não podemos saber qual é a senha do usuário e devemos confiar na política.

Um pentester irá testar essa política e ver se não já como descobrir a senha de algum funcionário de forma fácil, sendo assim, realizando um trabalho mais completo.

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Fanpage: www.facebook.com/academiahacker